Electronic Version

Stylesheet Version v1.1.1

Description

Classification of wanted e-mail via web of relationship utilization of Public Key Infrastructure (PKI)

Cross Reference To Related Applications

[0001] This application depends upon the patent application number 10/708,514, filed on 2004-03-09 at 13:59:39 EDT, titled "Reduction in unwanted e-mail (spam) through the use of portable unique utilization of public key infrastructure (PKI)". Specifically, the "Use of unique keys maintained by third party to end users for classification of email" in 10/708,514 allows for proper identification and use of friends lists. It is assumed that "Specific email server and client plug-ins to be developed to support portability" in 10/708,514 can and most likely will be the same as the those that provide the functionality for this invention.

Summary of Invention

[0002] Assuming that all email users are identified by a unique key, then an email system can take advantage of defined relationships.

[0003] An email system can record a list of friends, family and close associates. An incoming email can be forwarded to a specific folder or flagged for attention if it comes from someone in that list. Further it could be possible to delete all email from anyone not in that list.

[0004] Electronic mail needs to be able to serve as a human networking tool.

[0005] To support this, a user can specify "degrees of separation" for each trusted sender or utilize a general setting. Zero degrees of separation would have the effect of only allowing email from those specifically mentioned. One degree of separation would allow email from friends of friends. Delivery of e-mail is then subject to a web of relationship, just a communication in the real world.

[0006] A dynamic system of group keys will support encryption, if desired.

DETAILED DESCRIPTION

[0007] This invention depends on the establishment of identity of all senders and receivers in an e-mail system. This can be accomplished via a unique key for each user.

[0008] Users of this system will have the option of maintaining lists of friends, associates, family, etc. These lists will be used to categorize e-mail. The relationship of sender to the receiver of an email can cause the e-mail to be deleted, flagged for importance, ignored, placed in specific folders, or a combination of these options.

[0009] Users will have the option of maintaining a global setting for "degrees of separation" and/or maintaining the setting for individuals in the relationship lists.

[0010] "Degrees of Separation", denote the number of relationship links a sender can be separated from the receiver. Zero degrees of separation would have the effect of only allowing email from senders specifically mentioned in a relationship list. One degree of separation would allow email from friends of friends. Delivery of e-mail is then subject to a web of relationship, just as communication in the real world.

[0011] An unverified sender can be accepted, if the receivers rules allow it. Since an email that does not contain a unique key, could be forged, there is a risk that the message was unwanted. Further any "Degrees of Separation" greater than 0 would be risking even more unwanted email, if senders are not verified. Without a unique key it may also be difficult to reference the senders list of friends, limiting them zero "Degrees of Separation".

[0012] As in many e-mail clients and spam products, a user can specifically blacklist a sender, to prevent the delivery of email from that sender or to just remove any special treatment based on the web of relationship.

[0013] This invention can be seen as an enhancement of "Web of trust" as used by PGP. Please note that PGP may not be PKI algorithm used.

[0014] Users may have the need to send encrypted e-mail to multiple members of this web of relationship. To support this, the system will create upon need, a group key that is forwarded to each recipient.

[0015] These group keys will be sent utilizing the same method as in the patent application for 'Reduction in unwanted e-mail (spam) through the use of portable unique utilization of public key infrastructure (PKI)'.

[0016] The Group keys can have set validity periods. If a group key has expired, then the next attempt to send an encrypted e-mail will result in a new group key.

[0017] Group key validity periods and membership must be stored in e-mail servers.

[0018] If the group key itself is stored in servers, then additions to group membership can have the key forwarded to them.

[0019] Deletion from group membership, requires a new group key be created, otherwise the old group member could decrypt the message.

[0020] This method requires no decryption by any intermediary and prevents the need of encrypting for each recipient.